

IT-Sicherheits-Leitlinie

FOXIT
Version 1.2, 16.04.2009

Dokumentenbeschreibung:

Datei : \\FILE01\dfs\Units\ISO\FOXIT\Richtlinie-Leitlinie\FOXIT-Sicherheitsleitlinie.v1.2.docx
 Projekt : ISO 27001
 Seitenzahl : 6
 Erstelldatum : 21. Februar 2008
 Änderungsdatum : 16. April 2009

Historie

| Nr. | Datum | Autor | Kapitel | Änderungen | Version |
|-----|----------|----------------------|---------|------------------------------|---------|
| 1 | 21.02.08 | Christian Michlbauer | | | 1.0 |
| 2 | 16.06.08 | Christian Michlbauer | | Meßbare Ziele eingeführt | 1.1 |
| 3 | 16.04.09 | Christian Michlbauer | | Review – Meßbare Ziele 09/10 | 1.2 |

| | | |
|---|---------------------------|--|
| Freigabe: Hr. Obermayer Geschäftsleitung | Datum: <i>16.04.09</i> | Sign. FOX IT. think it - we make it F. Obermayer Datentechnik GmbH & Co. KG Edt. 4 84558 KIRCHWEIDACH |
|---|---------------------------|--|

TEL: +49 8623 98739-0 FAX: +49 8623 98739-33

MAIL: info@fox-it.de

Die Geschäftsführung verabschiedet hiermit folgende IT-Sicherheits Leitlinie als Bestandteil ihrer Strategie:

Stellenwert der Informationsverarbeitung

Informationsverarbeitung unterstützt unsere Aufgabenerfüllung und spielt eine wesentliche Rolle. Alle wesentlichen Funktionen und Aufgaben werden durch Informationstechnik (IT) maßgeblich unterstützt.

Ein Ausfall von IT-Systemen muss insgesamt kurzfristig kompensiert werden können.

Da unsere Kernkompetenzen in den Bereichen IT-Security Consulting, Datenschutz, IT-Service und Auftragsprogrammierungen liegen ist der Schutz dieser Informationen vor unberechtigtem Zugriff und vor unerlaubter Änderung ist von existenzieller Bedeutung.

Übergreifende Ziele

Unsere Daten sowie die Daten unserer Kunden und unsere IT-Systeme in allen Bereichen werden in ihrer Verfügbarkeit so gesichert, dass die zu erwartenden Stillstandszeiten toleriert werden können und keine wesentlichen Auswirkungen auf den Geschäftsbetrieb haben. Fehlfunktionen und Unregelmäßigkeiten in Daten und IT-Systemen sind nur in geringem Umfang und nur in Ausnahmefällen akzeptabel, die Gewährleistung der Integrität ist ein wichtiges Ziel. Die Anforderungen an Vertraulichkeit haben ein normales, an Gesetzeskonformität orientiertes Niveau.

IT-Sicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der schützenswerten Informationen und IT-Systeme stehen. Schadensfälle mit existenzbedrohenden finanziellen Auswirkungen (d.h. Auswirkungen von über [10%] des monatlichen Umsatzes) müssen verhindert werden.

Alle Mitarbeiter des Unternehmens halten die einschlägigen Gesetze (z. B. Strafgesetzbuch, Betriebsverfassungsgesetz, Handelsgesetzbuch, Sozialgesetzbuch, Gesetze und Regelungen zum Datenschutz) und vertraglichen sowie internen Regelungen ein. Negative finanzielle und immaterielle Folgen für das Unternehmen sowie für die Mitarbeiter durch Gesetzesverstöße sind zu vermeiden.

Alle Mitarbeiter und die Geschäftsleitung sind sich ihrer Verantwortung beim Umgang mit IT bewusst und unterstützen die IT-Sicherheitsstrategie nach besten Kräften.

Detailziele

Die Datenschutzgesetze und die Interessen unserer Mitarbeiter verlangen eine Sicherstellung der Vertraulichkeit der Mitarbeiterdaten. Die Daten und die IT-Anwendungen der Personalabteilung werden daher einem normalen Vertraulichkeitsschutz unterzogen. Gleiches gilt für die Daten unserer Kunden und Geschäftspartner.

Die Geschäftsabwicklung darf nicht verzögert oder gar gefährdet werden. Wenn vertraglich festgelegte Lieferfristen nicht eingehalten werden können, kann dies weitreichende negative Folgen haben. Insbesondere eine mangelhafte Verfügbarkeit der IT-Systeme und der Daten, aber auch Fehlfunktionen können zu Erlösminderungen führen und Vertragsstrafen nach sich ziehen.

Innerhalb der Produktionsabteilung wird die Verfügbarkeit und die Fehlerfreiheit der Systeme sichergestellt. Ausfallzeiten von IT-Systemen innerhalb der Produktion sind nur in einem geringen Maße akzeptabel, da diese direkt, aber auch indirekt durch negative Auswirkungen auf nachfolgende Prozesse – zu Erlösminderungen und Vertragsstrafen führen können.

Die Nutzung des Internets zur Informationsbeschaffung und zur Kommunikation ist für uns selbstverständlich und für die Kommunikation mit Kunden und Geschäftspartnern wesentlich. E-Mail dient als Ersatz oder als Ergänzung von anderen Bürokommunikationswegen. Durch entsprechende Maßnahmen wird sichergestellt, dass die Risiken der Internetnutzung möglichst gering bleiben.

Meßbare Ziele

Um die Wirksamkeit des Informations Sicherheits Prozesses messen zu können wurden meßbare Ziele definiert, deren Ergebnis als Input für den Managementreview an die Geschäftsführung dient.

Folgende Ziele wurde für den Berichtszeitraum 2009/2010 definiert:

- Die Reaktionszeiten auf Incident und Problem Tickets sind mit dem neuen Ticketsystem meßbar und konnten auf ca. 30 Minuten reduziert werden – dieser Wert gilt weiter einzuhalten.
- Die Reaktionszeiten auf Alerts und Events konnten durch den Einsatz des Monitoringsystems von derzeit mehreren Stunden auf 30 Minuten reduziert werden – diesen Wert gilt es einzuhalten
- Alle vertraulich eingestufen E-Mails müssen verschlüsselt werden – diese 100% Marke gilt es weiter einzuhalten.
- Die Schulungsmaßnahmen wurden zu einem großen Anteil ausgeweitet – auch die EntwicklungsSOPs müssen generell geprüft werden. Diese 100% Regelung hat sich bewährt und muss eingehalten werden.
- Alle sicherheitsrelevanten Prozesse müssen in FOXForward eingepflegt werden.
- Visualisierung der sicherheitsrelevanten Prozesse.
- Abbildung der Prozesse HR in Foxforward
- Erweiterung nach Tittmoning ohne Einschränkung für die Sicherheit.
- Mehr Redundanz durch die Erweiterung nach Tittmoning

IT-Sicherheitsmanagement

Zur Erreichung der IT-Sicherheitsziele wurde ein IT-Sicherheitsbeauftragter benannt. Der IT-Sicherheitsbeauftragte ist für die Erstellung und Fortschreibung des Sicherheitskonzepts sowie die Aufrechterhaltung des Sicherheitsniveaus verantwortlich. Er berichtet in seiner Funktion direkt an die Geschäftsleitung.

Dem IT-Sicherheitsbeauftragten werden von der Leitung ausreichende finanzielle und zeitliche Ressourcen für die Ausübung seiner Tätigkeit zur Verfügung gestellt. Er ist durch die IT-Verantwortlichen und IT-Benutzer ausreichend zu unterstützen und frühzeitig in alle Projekte einzubinden, um schon in der Planungsphase sicherheitsrelevante Aspekte zu berücksichtigen. Gleiches gilt, sofern personenbezogene Daten betroffen sind.

Die IT-Verantwortlichen und IT-Benutzer haben sich in sicherheitsrelevanten Fragestellungen an die Anweisungen des IT-Sicherheitsbeauftragten zu halten.

Sicherheitsmaßnahmen

Für alle Verfahren, Informationen, IT-Anwendungen und IT-Systeme wird eine verantwortliche Person benannt, die den jeweiligen Schutzbedarf bestimmt und Zugriffsberechtigungen vergibt.

Für alle verantwortlichen Funktionen sind Vertretungen einzurichten. Es muss durch Unterweisungen und ausreichende Dokumentationen sichergestellt werden, dass Vertreter ihre Aufgaben erfüllen können.

Gebäude und Räumlichkeiten werden durch ausreichende Zutrittskontrollen geschützt. Der Zugang zu IT-Systemen wird durch angemessene Zugangskontrollen und der Zugriff auf die Daten durch ein angemessenes Berechtigungskonzept geschützt.

Computer-Viren-Schutzprogramme werden auf allen IT-Systemen eingesetzt. Alle Internetzugänge werden durch eine geeignete Firewall gesichert. Alle Schutzprogramme werden so konfiguriert und administriert, dass sie einen effektiven Schutz darstellen und Manipulationen verhindert werden. Des Weiteren unterstützen die IT-Benutzer durch eine sicherheitsbewusste Arbeitsweise diese Sicherheitsmaßnahmen und informieren bei Auffälligkeiten den IT-Sicherheitsbeauftragten.

Datenverluste können nie vollkommen ausgeschlossen werden. Durch eine Datensicherung wird daher gewährleistet, dass kurzfristig verlorene oder fehlerhafte Teile des operativen Datenbestandes wiederhergestellt werden

können. Informationen werden einheitlich gekennzeichnet und so aufbewahrt, dass sie schnell auffindbar sind.

IT-Benutzer nehmen mindestens jährlich an einer internen Sicherheitsunterweisung durch den IT-Sicherheitsbeauftragten teil.

Verbesserung der Sicherheit

Das IT-Sicherheitskonzept wird regelmäßig auf seine Aktualität und Wirksamkeit geprüft.

Die Geschäftsleitung unterstützt die ständige Verbesserung des Sicherheitsniveaus. Mitarbeiter sind angehalten, mögliche Verbesserungen oder Schwachstellen an den IT-Sicherheitsbeauftragten weiterzugeben.

Durch eine kontinuierliche Revision der Regelungen und deren Einhaltung wird das angestrebte Sicherheits- und Datenschutzniveau sichergestellt.

Abweichungen werden mit dem Ziel analysiert, die IT-Sicherheitssituation zu verbessern und ständig auf dem aktuellen Stand der IT-Sicherheitstechnik zu halten.